	COUNTY OF SAN BERNARDINO STANDARD PRACTICE	No. 2-366SP Effective: July 10, 2006 By: Bea Valdez, Interim Chief of Administrative Services	Issue No. 1 Page 1 of 3
	PUBLIC HEALTH	Approved: James A. Felten Public Health Director	
Subject: TRANSMISSION SECURITY			

I. POLICY

The Department of Public Health (DPH) must protect the confidentiality of sensitive information at all times by taking reasonable precautions when transmitting (sending or receiving) information, in accordance with Department, County, State and Federal requirements.

II. PURPOSE:

This standard practice establishes guidelines for DPH workforce members for the secure transmission (sending and receiving) of sensitive information.

III. SCOPE:

A. Workforce Members must:

1. Ensure sensitive information is adequately protected at all times.
2. Have reasonable assurance that the receiver is authorized to view the information and that the receiver's identity has been validated.
3. Ensure that all transmitted disclosures of protected health information are documented.

B. Program Managers or Designees must periodically spot check transmissions of sensitive information to and from their programs.

IV. TRANSMISSION PROCEDURES:

A. E-mail Transmissions

E-mail is permissible to the extent that the e-mail is necessary to conduct healthcare operations and only the minimum necessary information is sent. If possible, confidential information should not be sent using e-mail.

1. All e-mail containing sensitive information must include a confidentiality statement in the body of the e-mail (see sample below).

   > *The information contained in this e-mail is legally privileged and confidential information intended only for the use of the individual or entity to whom it is addressed. If the reader of this message is not the intended recipient, you are hereby notified that any viewing, dissemination, distribution, or copy of this e-mail message is strictly prohibited. If you have received and/or are viewing this e-mail in error, please immediately notify the sender by reply e-mail, and delete this e-mail from your system.*

2. All e-mail transmissions containing sensitive information must be followed up with a phone call to make sure the intended party received the transmission.
3. Sensitive information sent by e-mail as a Microsoft Office document (Word or Excel) should be password-protected as follows:

   Word Documents:

   a. On the "Tools" menu, click "Protect Document," type a password, click "OK."

b. Confirm password in the pop-up box by retyping the password and click "OK."

c. Save the file and attach to the e-mail.

Excel Documents

a. On the "Tools" menu, click "Protection" then "Protect Workbook."

b. Type a password; click "OK."

c. Confirm password in the pop-up box by retyping the password and click "OK."

d. Save the file and attach to the e-mail.

Internal Transmissions

1. Sensitive information sent within the County of San Bernardino should be sent as an attachment, not displayed in the body of the e-mail.
2. When the document is password-protected, the password should be sent in a separate e-mail or disclosed to the requestor via a follow-up telephone call.

External Transmissions

1. If transmission is to a non-County entity, sensitive information must be encrypted utilizing digital certification or by encrypting the attachment utilizing third party software.
2. Contact your Information Technology (IT) automated systems analyst for more information or assistance.
3. De-encryption information must be communicated to the receiver in a separate e-mail or via a follow-up telephone call.

B. **Text-Based Paging Systems**

Sending sensitive information using E-mail or Internet text-based paging systems is restricted to emergency paging only and should be used only as a last resort when no other options exist.

C. **Removable media**

Sensitive information must be protected when, stored, copied, transmitted, or transported using any type of removable media.

Removable media includes items such as floppy disks, CDs and any technology device capable of sending, receiving or storing electronic data. (For a list of removable media, see Policy 2-360, Device and Media Controls.) Permitted use of such devices requires the following:

1. Use encryption software or password to protect against unauthorized access to protected health information (PHI).
2. If using removable media for the purpose of systems backup and disaster recovery and the removable media is used in a secure manner and stored or transported securely, no additional security mechanisms are required.

D. **Facsimile**

1. Use a coversheet that labels the transmission as confidential.
2. Confirm that the fax number used is correct prior to transmission.
3. Ensure the fax machine is in a secure location.
4. Before faxing, telephone the recipient to alert them that the fax is being sent.

V. TRANSMISSION SECURITY METHODS

IT will use the following transmission security methods as needed:

A. **Virtual Private Network (VPN)**

A network that uses the Internet as the medium for transporting data by using public wires to connect nodes. These systems use encryption and other security mechanisms to ensure that only authorized users can access the network, and that the data cannot be intercepted.

B. **Secure Sockets Layer (SSL) encryption**

A protocol developed for transmitting private documents via the Internet using cryptographic keys (a public key known to everyone and a secret key known only to the message recipient) to encrypt data.

C. **Secure Web/FTP Server**

An alternative method for transmission is a secure web server to house sensitive information. The recipient is notified by E-mail that their information is available on a website requiring a user ID and password for access.

VI. VIOLATIONS:

Failure to comply with this policy may result in disciplinary action up to and including termination of employment/contract.

VII. REFERENCE:

Related Policies

1. 2-366, Transmission Security
2. 2-360, Device and Media Controls